Über das cubische Reciprocitätsgesetz.

Von **L. Gegenbauer.**

Bezeichnet man die elliptische Function $p(u; 0, 1)$, welche die complexe Multiplication mit Zahlen von der Form $a+b\rho$, wo ρ eine primitive dritte Einheitswurzel ist, zulässt, mit $p(u)$, ein primitives Periodenpaar derselben mit 2ω, $2\omega'$ und versteht unter m und n zwei ungerade primäre Primzahlen von der Form $a+b\rho$, so ist

$$\prod_{\lambda} p\left(\frac{2\lambda\omega}{m}\right) = -\frac{1}{m^{\frac{1}{3}}},$$

wo λ ein Sechstelrestensystem nach dem Modul m durchläuft und $m^{\frac{1}{3}}$ eine bestimmte dritte Wurzel aus m ist.

Es ist nun

$$\prod_{\lambda} \left(\frac{p\left(\frac{2n\lambda\omega}{m}\right)}{p\left(\frac{2\lambda\omega}{m}\right)}\right)^2 = \left[\frac{n}{m}\right],$$

wo $\left[\frac{n}{m}\right]$ das von Eisenstein für den cubischen Charakter einer durch m nicht theilbaren Zahl n eingeführte Zeichen ist.

Man hat daher:

$$\prod_{\lambda} \left(p\left(\frac{2n\lambda\omega}{m}\right)\right)^2 = \left[\frac{n}{m}\right] m^{-\frac{2}{3}}$$

oder weil $p\left(\frac{2n\lambda\omega}{m}\right)$ eine rationale Function von $p\left(\frac{2n\omega}{m}\right)$ ist:

$$G\left(p\left(\frac{2n\omega}{m}\right)\right) - \left[\frac{n}{m}\right] m^{-\frac{2}{3}} G_1\left(p\left(\frac{2n\omega}{m}\right)\right) = 0.$$

Bekanntlich zerfallen alle durch m nicht theilbaren Reste in drei Gruppen, je nachdem $\left[\frac{n}{m}\right] = 1, \rho, \rho^2$ ist, und werden die Zahlen der ersten Gruppe die cubischen Reste von m genannt. Bezeichnet man die Zahlen der $\varkappa^{\text{ten}}$ Gruppe mit $a_{\varkappa,\tau}$, so sind die die Grössen $\gamma\left(\frac{2a_{\varkappa,\tau}\omega}{m}\right)$ Wurzeln der Gleichung:

$$H_\varkappa(x) = G(x) - \rho^{\varkappa-1} m^{-\frac{2}{3}} G_1(x) = 0.$$

Setzt man:

$$\frac{p(mu)}{p(u)} = \frac{\Phi([p(u)]^2)}{\Psi([p(u)]^2)},$$

so folgt aus der letzten Bemerkung, dass die Functionen $H_1(x)$ und $\Psi(x^2)$ einen gemeinsamen Theiler haben. Der grösste gemeinsame Theiler der eben genannten Functionen ist, wie man sofort sieht, die Function

$$\prod_\tau \left(x - p\left(\frac{2a_{1,\tau}\omega}{m}\right)\right),$$

wo sich das Product über ein System von incongruenten Grössen $a_{1,\tau}$ erstreckt.

Da die Coëfficienten von $\Psi(x^2)$ ganze complexe Zahlen von der Form $a+b\rho$ sind, welche mit Ausnahme des letzten, der gleich $(-1)^{\frac{\text{Norm } m-1}{3}}$ ist, durch m theilbar sind, da ferner die Coëfficienten von $H_1(x)$ von $m^{-\frac{2}{3}}$ abhängen, so sind die Coëfficienten des grössten gemeinsamen Theilers ganze aber nicht nothwendig auch ganzzahlige Functionen von ρ und $\sigma = m^{-\frac{2}{3}}$.

Betrachtet man die drei Gleichungen, welche der analytische Ausdruck des Vorhandenseins des grössten gemeinsamen Theilers zweier Functionen sind, berücksichtigt man ferner, dass eine Gleichung, welche für eine Wurzel einer irreductiblen Gleichung besteht, für alle Wurzeln derselben bestehen muss, so sieht man, dass unter der Voraussetzung, dass die Gleichung $y^3 = m^{-2}$ irreductibel ist — eine Voraussetzung, welche im vorliegenden Falle sicher erfüllt ist — $\Psi(x^2)$ unter Adjunction von σ in drei Factoren zerfällt, welche passend mit $\varphi(x, \sigma)$, $\varphi(x, \rho\sigma)$ und $\varphi(x, \rho^2\sigma)$

bezeichnet werden können. Dass $\Psi(x^2)$ sich unter Adjunction von σ nicht weiter zerlegen lässt, folgt aus dem Umstande, dass diese Function, wie Dantscher gezeigt hat, im gewöhnlichen Sinne irreductibel ist.

Wir haben also eine Gattung von Functionen gefunden, unter deren Adjunction eine in der Theorie der von uns behandelten speciellen elliptischen Functionen auftretende Gleichung reductibel wird. Eine allgemeine Untersuchung über die Eigenschaften derjenigen Gattungen von algebraischen Functionen, unter deren Adjunction die in der Theorie der elliptischen Functionen auftretenden Gleichungen reductibel werden, ist meines Wissens bisher noch nicht veröffentlicht worden und doch dürfte die Kenntniss dieser Eigenschaften für manche Fragen, z. B. für die Reduction der Integrale etc., von nicht geringer Bedeutung sein.

Ist nun $S\left(p\left(\frac{2a_{\varkappa_1\tau}\omega}{m}\right)\right)$ eine ganze symmetrische Function der $\frac{\text{Norm}\, m-1}{3}$ Grössen $p\left(\frac{2a_{\varkappa_1\tau}\omega}{m}\right)$, welche man erhält, wenn man für die Werthe $a_{\varkappa_1\tau}$ ein System von incongruenten Zahlen $a_{\varkappa_1}$ setzt, so folgt aus den elementarsten Sätzen über symmetrische Functionen, dass:

$$S\left(p\left(\frac{2a_{\varkappa_1\tau}\omega}{m}\right)\right) = A + B\rho^{\varkappa-1}\sigma + C\rho^{2\varkappa+1}\sigma^2 \quad [\varkappa = 1, 2, 3]$$

ist, wo A, B, C ganze aber nicht nothwendig ganzzahlige Functionen von ρ sind. Aus diesen Gleichungen folgt:

$$\sum_{\varkappa=1}^{\varkappa=3} \rho^{2\varkappa+1} S\left(p\left(\frac{2a_{\varkappa_1\tau}\omega}{m}\right)\right) = 3B\sigma.$$

Diese Gleichung liefert, wie man sieht, eine Darstellung von dritten Wurzeln durch elliptische Functionen.

Setzt man Norm $n = \nu$, so folgt aus der letzten Gleichung:

$$\sum_{\varkappa=1}^{\varkappa=3} \rho^{2\varkappa+1} S^{\nu}\left(p\left(\frac{2a_{\varkappa_1\tau}\omega}{m}\right)\right) \equiv D^{\nu}\sigma^{\nu} \pmod{\nu},$$

wo $3B = D$ gesetzt wurde. Unter Berücksichtigung des Fermat'schen Satzes lässt sich diese Relation auch in folgender Form schreiben:

$$\sum_{\varkappa=1}^{\varkappa=3} \rho^{2\varkappa+1} S\left(\left[p\left(\frac{2a_{\varkappa,\tau}\omega}{m}\right)\right]\right) \equiv D^{\nu}\sigma^{\nu} \pmod{\nu}.$$

Da aus der Gleichung:

$$p(nu)\,\{n[(p(u))^{\frac{\nu-1}{2}} + c_1(p(u))^{\frac{\nu-5}{2}} + \cdot \qquad] + (-1)^{\frac{\nu+5}{6}}\}^2 =$$
$$= p(u)\,\{p(u)^{\nu-1} + n\,[cp(u)^{\nu-5} + \ldots]\}$$

folgt:

$$p\left(\frac{2na_{\varkappa,\tau}\omega}{m}\right) \equiv \left(p\left(\frac{2a_{\varkappa,\tau}\omega}{m}\right)\right)^{\nu} \pmod{n},$$

so ergibt sich aus der letzten Relation die Congruenz:

$$\sum_{\varkappa=1}^{\varkappa=3} \rho^{2\varkappa+1} S\left(p\left(\frac{2na_{\varkappa,\tau}\omega}{m}\right)\right) \equiv D^{\nu}\sigma^{\nu} \pmod{n}.$$

Berücksichtigt man, dass:

$$\left[\frac{\alpha\,.\,\beta}{m}\right] = \left[\frac{\alpha}{m}\right]\cdot\left[\frac{\beta}{m}\right]$$

ist, so kann man diese Congruenz auch in folgender Form schreiben:

$$\left[\frac{n}{m}\right] \sum_{\varkappa=1}^{\varkappa=3} \rho^{2\varkappa+1} S\left(p\left(\frac{2a_{\varkappa,\tau}\omega}{m}\right)\right) \equiv D^{\nu}\sigma^{\nu} \pmod{n}$$

oder:

$$\left[\frac{n}{m}\right] D\,.\,\sigma \equiv D^{\nu}\sigma^{\nu} \pmod{n}.$$

Die Grösse D hängt von der Wahl der symmetrischen Function S ab. Ist nun S so gewählt, dass D eine durch n nicht theilbare ganze complexe Zahl von der Form $a + b\rho$ ist — dass dies möglich ist, folgt aus den im Anfange angeführten Gleichungen — so folgt aus dieser Congruenz:

$$\left[\frac{n}{m}\right] \equiv \sigma^{\nu-1} \pmod{n}$$

oder:

$$\left[\frac{n}{m}\right] \equiv \left[\frac{m}{n}\right] \pmod{n}.$$

Aus dieser Congruenz folgt bei den gemachten Voraussetzungen sofort:

$$\left[\frac{n}{m}\right] = \left[\frac{m}{n}\right].$$

Hiermit ist das cubische Reciprocitätsgesetz für ungerade primäre Primzahlen von der Form $a+b\rho$ bewiesen.

Es mag noch schliesslich bemerkt werden, dass das Reciprocitätsgesetz für die sechsten Potenzreste sich mit Hilfe derselben Function $p(n;\, 0,\, 1)$ leicht beweisen lässt.